OpenAM 10.20 Snapshot版

新機能紹介

OSSTech

2013年4月12日

オープンソース・ソリューション・テクノロジ株式会社

http://www.osstech.co.jp/

お問い合わせ info@osstech.co.jp

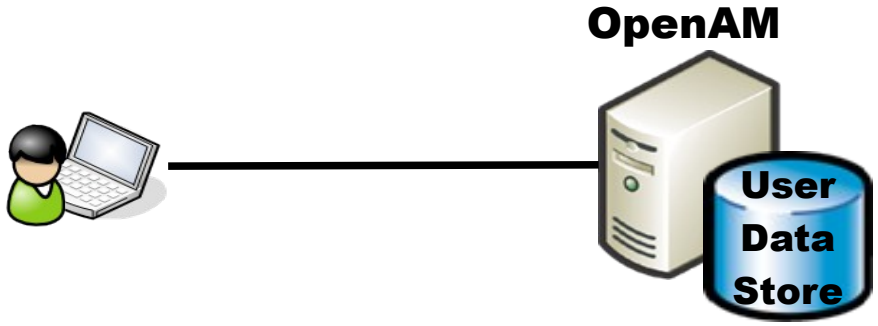
今回注目の機能

- セッション・フェイルオーバーの改良
  - 設定が飛躍的に容易になった
  - OpenDJのレプリケーション機能を使用
- OATH準拠した認証方式の追加
  - Googleの２段階認証と同じ仕組み
  - 強固な認証を安価に実現可能
- OAuthプロバイダのサポート
  - OpenID Connectに向けた基盤の準備

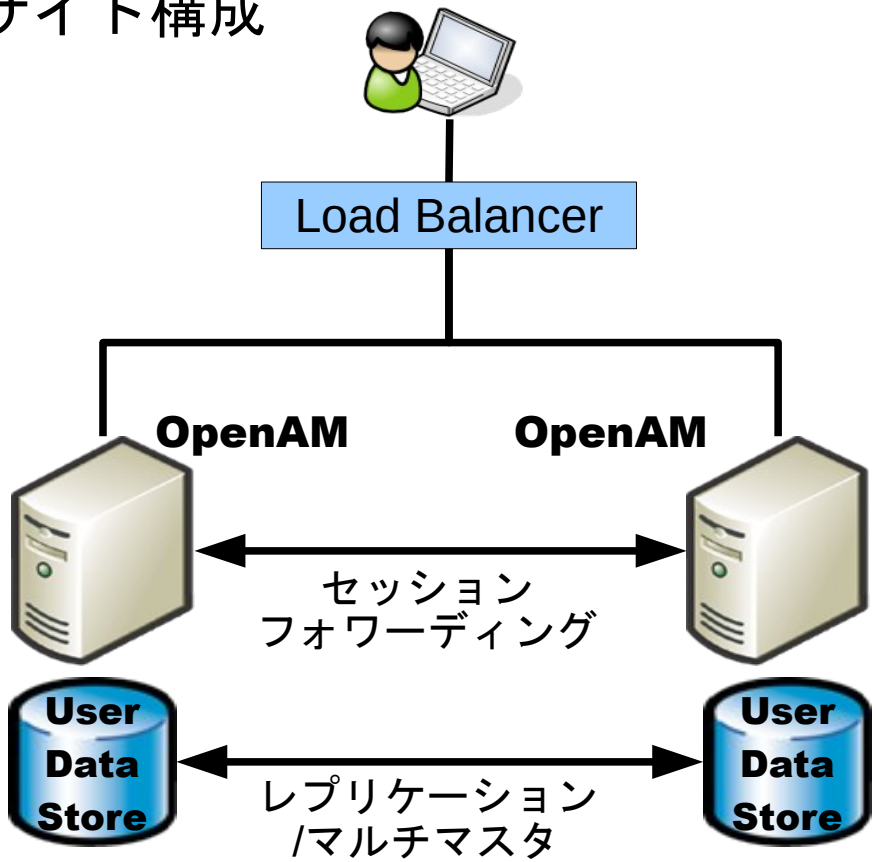
セッション・フェイル・オーバー(SFO)の改良

OpenAMの冗長化構成

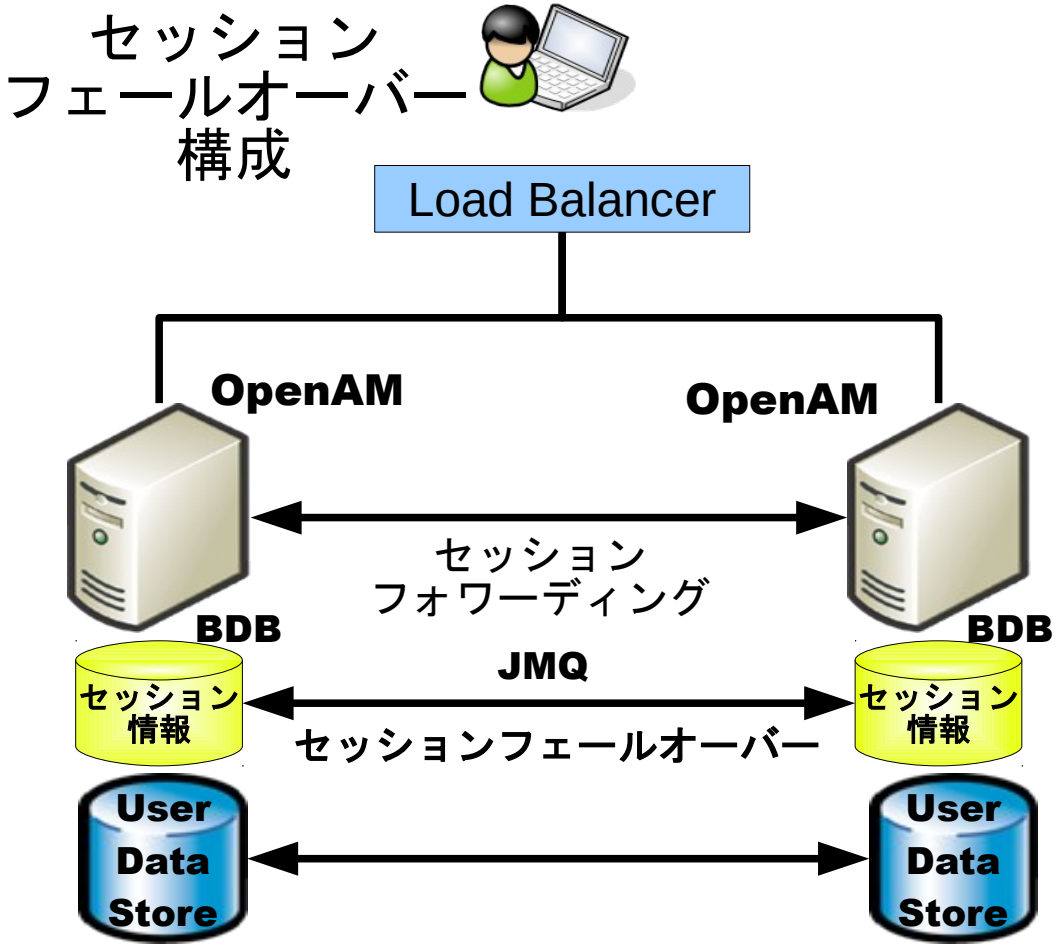
シングルサーバ構成



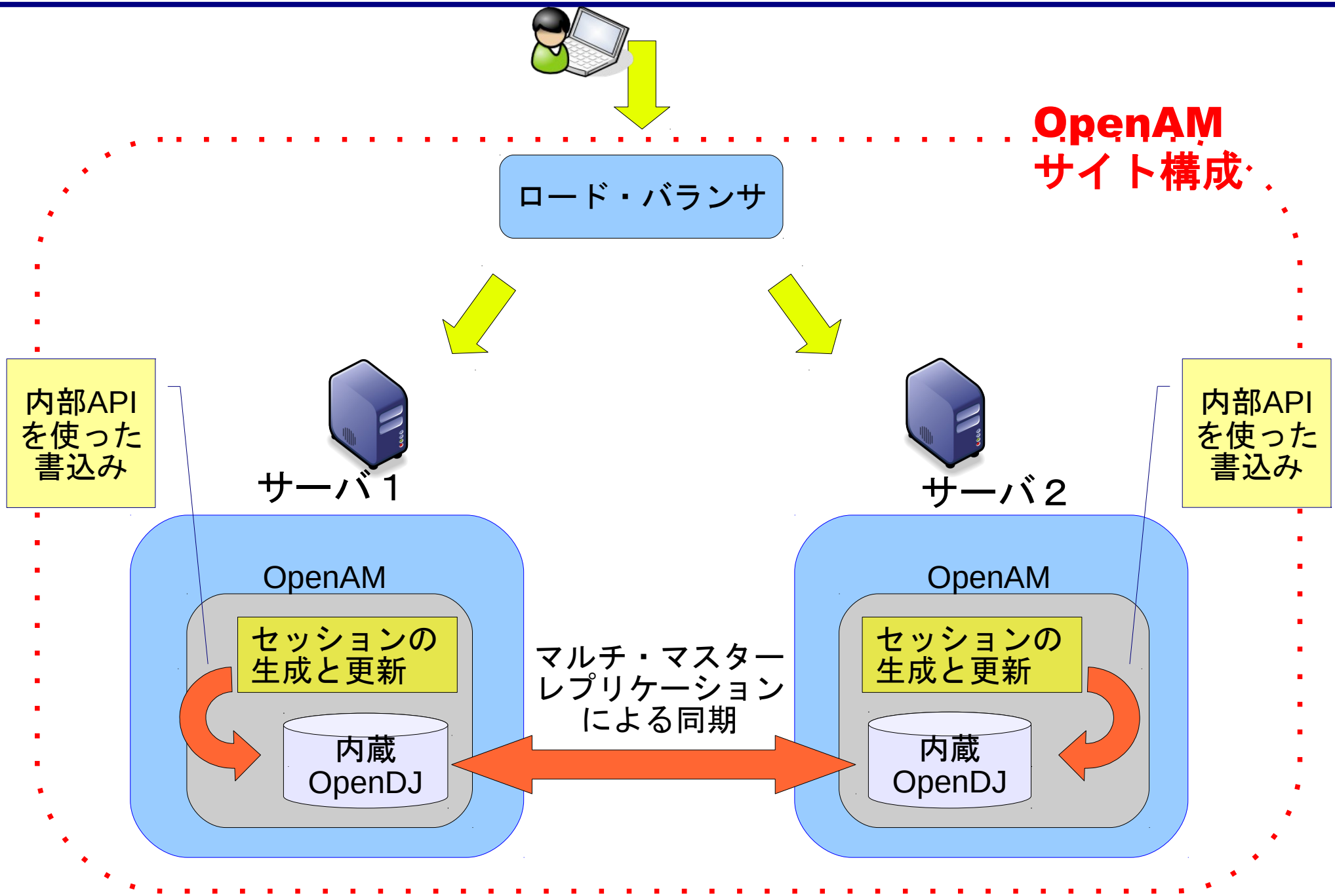
サイト構成



セッション フェールオーバー 構成



新しいセッション・フェイルオーバーの仕組み



OpenDJを使ったセッションの永続化

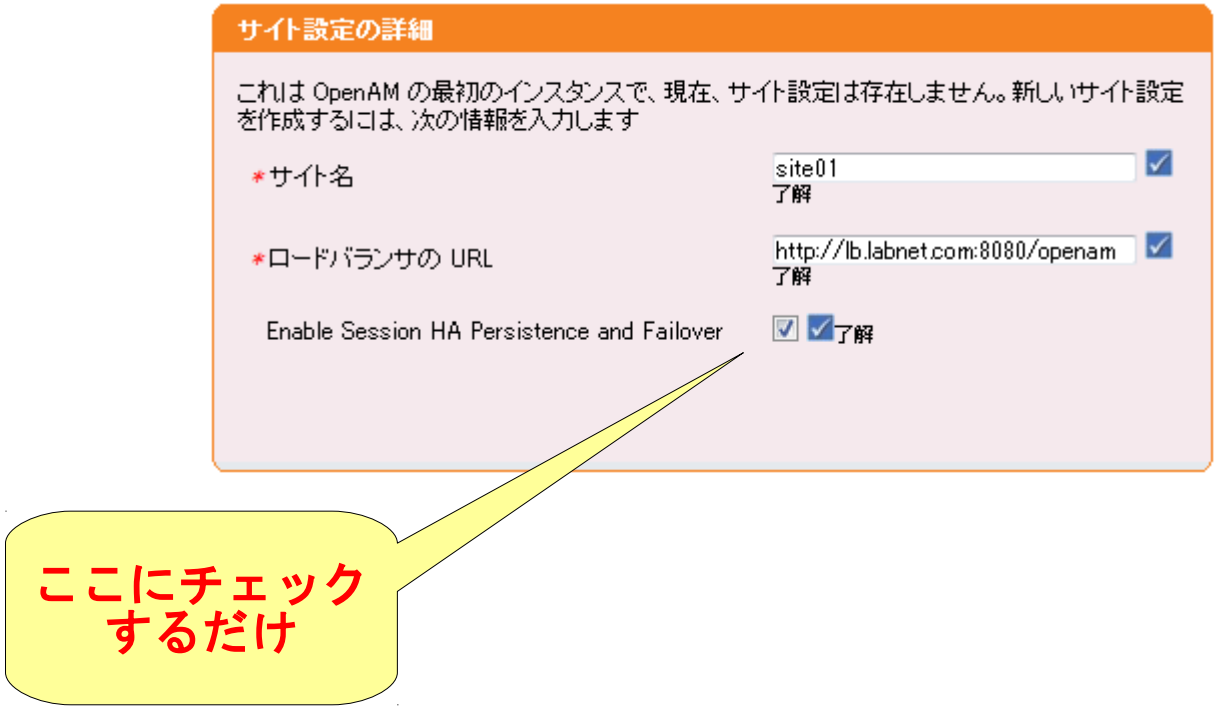
- 内蔵OpenDJへのセッション情報の書込み
  - サイト構成の場合に設定オプションとして利用可能
  - メモリ上のセッションテーブルも引き続き利用（自分で発行したもののみ）
  - 再起動した場合には、OpenDJからセッション情報を読込み再構成する
- マルチ・マスタ・レプリケーションによるセッションの冗長化
  - 他のサーバが停止した場合は、そのサーバのセッション情報をOpenDJからメモリ上に再構成しサービスを引き継ぐ

構成が単純でスケールする

- 難しいことはOpenDJに任せよう！
  - 複数台のサーバにわたるセッションの同期はDirectory サーバのマルチマスタ・レプリケーション機能で解決
  - メッセージキュー、Berkeley DBは必要無し！
  - OpenAMは必要なセッション情報は全てローカルにあるものとして動作
    （個人毎のセッション数の上限値など未実装もあり）
- OpenDJの高い更新性能を利用
  - 内蔵OpenDJ（同じJVM上で動作）へは内部APIを使ってアクセス（ディフォルト設定ではログに出ないので注意！）
  - マルチマスタ・レプリケーション処理の効率化

設定も簡単

- インストール時に指定



OpenDJの更新性能

- Benchmark proves OpenDJ fastest directory server !

  （Ludoのブログから引用）

  - 第三者による評価(M-Vault)

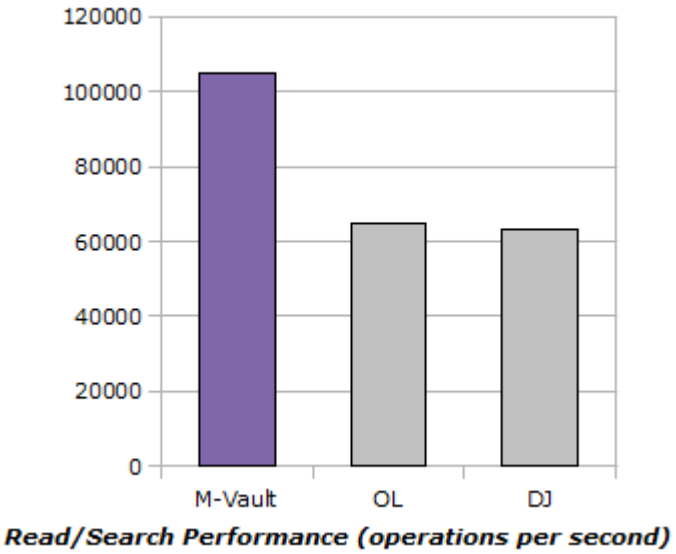
    http://www.isode.com/whitepapers/m-vault-benchmarks.html

  - 内部APIを使った場合はもっと速い（と思われる）

	Modify only (ops/sec)	Search - Modify (ops/sec)	
		Search	Modify
M-Vault	5,000	85,000	3,000
OpenLDAP	7,800	49,000	3,400
OpenDJ	10,000	55,000	4,200

- ところで検索性能は？

  - M-Vaultが最速
  - 本当に必要かな？？



OATHとyubikeyへの対応

オープンな認証仕様(**O**pen **A**u**TH**entication)

２種類のワンタイム・パスワード方式

- TOTP　ー　時刻ベース
  - 一定間隔（default: 30 sec) で新しいパスワードを生成
  - カウンタ：時刻
- HOTP　ー　イベント（カウンタ）・ベース
  - ログインの度に新しいパスワードを生成
  - カウンタ：生成回数

様々なサービスが認証強化のために

ワンタイム・パスワードを採用

- Google ： ２段階認証
  - メール、アプリ、電話、予備用のパスワード発行
- facebook：ログイン承認
  - メール、アプリ
- Yahoo! Japan：ワンタイム・パスワード
  - メール、アプリ
- Apple ： 日本ではこれから導入予定

安価で安全、しかも簡単！

- 標準化されたトークン・アプリの利用
  - スマートフォン上で動作、新たに購入する必要無し
  - OATH準拠のものなら何でもＯＫ
    - Google Authenticator (Google認証システム)
    - Android Tokenなど
- ２段階認証を簡単に実現
  - 落としても大丈夫
  - OpenAMの認証連鎖を使って簡単に構築
- yubikey等のハードウェアトークンもサポート

OpenAMの２段階認証

- 第１段階：ユーザIDとパスワードで認証

- 第２段階：ワンタイム・パスワードで認証

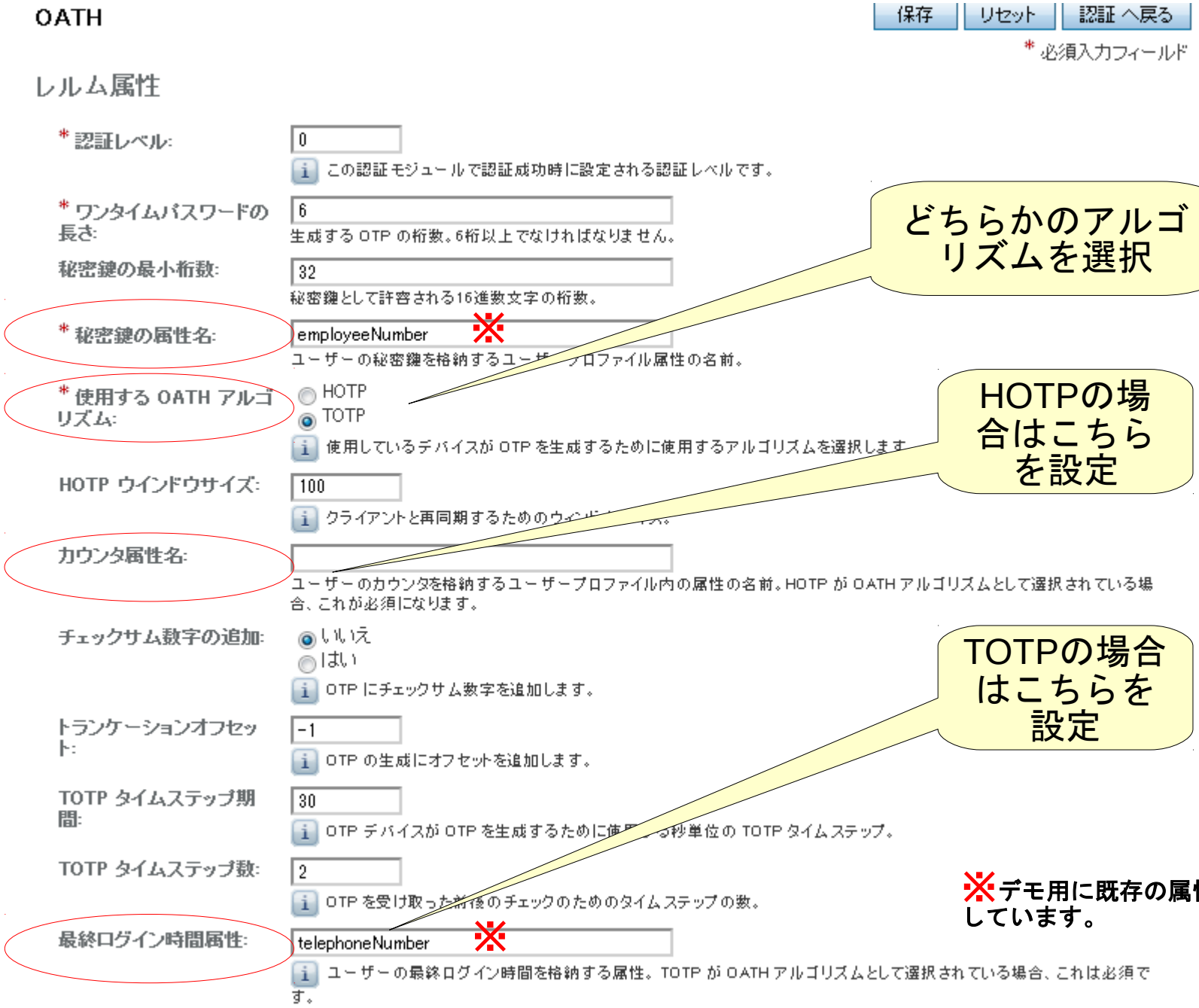
OpenAMで出来ること

- TOTP, HOTPの両方に対応
  - メールおよびOATH準拠のデバイスをサポート
  - 電話、予備用パスワードの発行は出来ない
- 他の認証方式との組合せが可能
  - アタプティブ・リスク認証との組合せ
  - 認証レベルによるアクセス制御
- 初期データの同期は別途必要
  - 共通シークレットをデバイスとサーバのそれぞれに配布、設定する必要あり
  - ＱＲコードを生成してスキャンさせる方法がお勧め

OpenAMの設定

- OATH認証モジュールの設定
  - 秘密鍵の属性名
  - 使用する OATH アルゴリズム ：HOTPまたはTOTPを選択
  - カウンタ属性名（HOTPのみ）
  - 最終ログイン時刻属性名（TOTPのみ）
- 認証連鎖の設定
  - 第１段階：Datastore認証(ユーザID/パスワード)
  - 第２段階：OATH認証
- メールを使う場合は従来と同様(HOTP認証）を使う
  - メールを使うHOTP認証は別モジュールになっているため注意！

OpenAM：OATH認証モジュールの設定



ユーザデータの設定

- 共通シークレットの設定
  - ランダムに生成されたバイナリデータ
  - 「秘密鍵の属性」に１６進数表示で設定
  - 長さは２０バイト（５の倍数）がお勧め（Googleは１０バイト）
- カウンタ/時刻の初期値
  - “1”を設定　（空だとダメ）

デバイスの設定

- 共通シークレット
  - 20 バイトのバイナリデータ：１６進数表示
  - 例：61626364656162636465616263646561626364 65
- Base32に変換

  例：MFRGGZDFMFRGGZDFMFRGGZDFMFRGGZDF
- 以下のURI形式にフォーマット

  otpauth://totp/<ラベル>?secret=<Base32の値>

  例：otpauth://totp/r1user1?secret=MFRGGZDFMFRGGZDFMFRGGZDFMFRGGZDF
- QRコードに変換
- 認証アプリでスキャン

yubikeyの紹介

- Yubicoにより開発
  - 本社：スウェーデン
- USBインターフェイス
  - キーボード・ディバイスとして認識される
  - パスワードを手で入力する必要がない
- 時計は内蔵していない
  - 単独でTOTPは不可
  - 安価で長持ち
- 関連モジュールをオープンソースで提供
  - OpenAMとの相性が良い

ダウンロードのお勧め

- OpenAMはユーザのニーズを取り込むことにより着実に進化しています。
- 今回、紹介した機能は、簡単に試してみることが可能です。
- 是非、ダウンロードして使ってみて下さい。

オープンソース・ソリューション・テクノロジ株式会社
http://www.osstech.co.jp/
お問い合わせ *info@osstech.co.jp*